

RapidMiner-based Clustering Techniques for Enhancing Intrusion Detection System (IDS) Performance

Johar Mumtaz^{1*}, Syed Asad Ali Naqvi¹, Muhammad Haroon Ahmad², Mudassar Rehman², and Gohar Mumtaz¹

¹Faculty of Computer Science and Information Technology, Superior University, Lahore, 54000, Pakistan

²Riphah International University, Lahore, 54000, Pakistan

*Corresponding Author: Johar Mumtaz. Email: joharmumtaz@gmail.com

Received: May 01, 2024 Accepted: August 13, 2024 Published: September 01, 2024

Abstract: Cybersecurity is the process of protecting networks, computers, servers, mobile devices, electronic systems, and data against hostile intrusions. It is the need of hour to be protected from the latest cyber-attacks. By examining traffic, Intrusion Detection Systems (IDS) assists in identifying possible dangers, unauthorized access, and unusual activity and notifies administrators to take appropriate action. Machine Learning (ML) clustering techniques are being used widely to make IDS better. In this research study, by utilizing clustering and classification techniques, such as Support Vector Machines (SVM), Boosting Naïve Bayes (BNB), K-Mean, and K-Medoids, the efficiency of the clustering techniques is examined. Further, we divided our research study in to cyber-attacks prediction and cyber-attacks detection categories. We used SVM and BNB clustering approaches for cyber-attacks prediction and compared the results. K-Mean and K-Medoids clustering approaches are used for cyber-attacks detection and the results are compared. Finally, we concluded that SVM is better approach for cyber-attacks prediction and K-Medoid is better approach for cyber-attacks detection.

Keywords: Cyber Security; Cyber Space; Intrusion Detection systems (IDS); Cyber-Attack Detection; Trespassing; Data Mining; Clustering; Machine Learning.

1. Introduction

Our lives are influenced by the most powerful invention of 20th century “The Internet “[1]. With the rapid expansion of the digital world, the Internet has become an indispensable part of modern life. According to the World Internet Statistics Report, the internet grew at a pace of 1.14 percent between 2000 and 2020, producing more than two quintillion bytes of data per day [2]. Internet addiction is growing as a result of the development of smart cities, self-driving cars, wearable health monitoring, mobile banking, AI robot systems, and many other technologies. Although these technologies greatly benefit people and communities, they also present a number of risks to personal data and operating systems [3].

The importance of data security makes it crucial for the development of intelligent cybersecurity systems and services. If sufficient cyber security in big data is not given priority, hackers may be able to obtain fast access to data that has been processed by technology. Hackers are always refining their strategies and developing dangerous software to take advantage of private information belonging to governments, businesses, and individuals. Cyberattacks are becoming more frequent despite strong security measures [4]. Cyber security NIST framework (shown in Fig. 1.) helps organizations to better interpret cyber security management.

As per the data of cyber-attack Fig. 2 shared by ISACA’s UK, Given the significant increase in data usage and internet activity, there is an urgent need to raise global awareness about cybersecurity [5].

Machine Learning (ML) algorithms may be used to efficiently handle and categorize the attacks [6]. Machine Learning plays an important role in cyber security by analyzing the dataset under different

techniques (shown in Fig. 3.). Machine Learning, Deep Learning, Block-chain, Data Mining and many more are the different terms which gives the cyber security a giant support. As, Federated Machine Learning (FML) gives us de-sterilized approach, Deep Learning algorithm helps us to figure out the attacks, Block-chain provides us the optimal solution against cyber-attacks and Data Mining techniques helps us to mine history data so, we can predict the next attack in the future and prevent them. Data mining techniques helps the clinical researcher to better understand the database technologies [7].

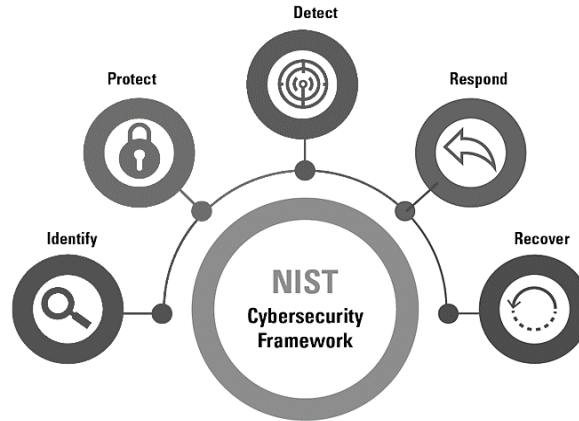


Figure 1. Cyber Security Framework

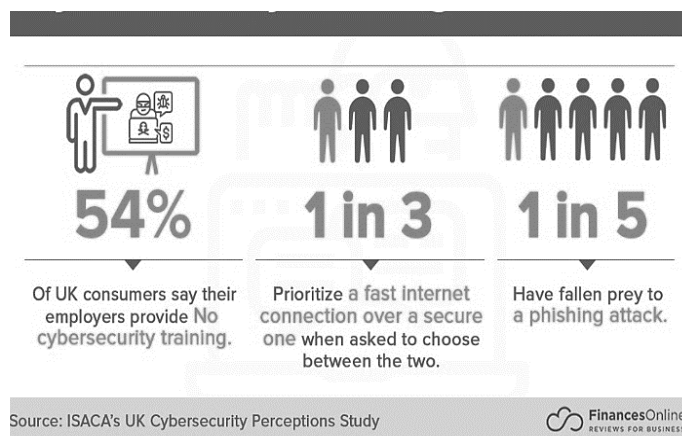


Figure 2. ISACA UK cybersecurity perception study

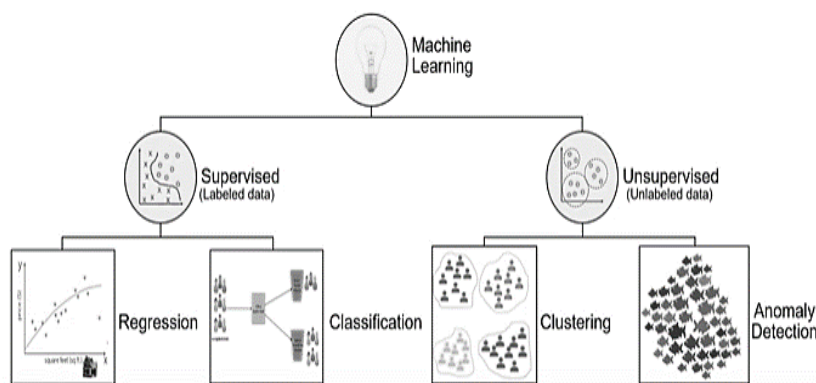


Figure 3. Machine Learning Techniques

In a big data, clustering techniques is interesting and key research area for researcher for detecting possible intrusions and trespassing in operating system. Intrusion detection refers to the process of monitoring computer networks or systems for malicious activities. As the cyberattacks are getting smarter day by day, intrusion detection is an emerging field for researcher to find new algorithm to shield the cyber security. Similarly, clustering methods can be used to analyze system logs for anomalous behavior. By clustering similar log entries together, the system can identify patterns and anomalies that may indicate a cyber-attack, such as unusual login attempts or unusual processes running on the system [8].

Clustering methods can be applied to analyze system logs and network traffic data in order to identify patterns and anomalies that may indicate a potential cyber-attack [9]. The motivation behind this is to compare well-known clustering method to find the best one. By Using the KDD99 Dataset [10], here we have compared the two well-known clustering approaches Boosting Naïve Bayes (BNB) Model [11] and Support Vector Machine (SVM) [12] used for cyber-attack prediction, in which SVM works more accurately. Also made a comparative discussion on K-Mean [13] and K-Medoid [14] clustering in which K medoids gives the best results for cyber-attack detection. Our research introduces a novel clustering method for detecting anomalous intrusions, which utilizes the K-medoids clustering approach and its specific adaptations. The newly proposed algorithm achieves a high detection rate and overcomes the limitations of the K-means algorithm. This will undoubtedly enhance system efficacy and accelerate the detection and prevention of attacks [42] [43].

In this paper Section II Listed the related work. Section III Describe the dataset KDD99 and methodology of work done. Further cyber-attack prediction and detection is compared and their results are shown in Section IV. Section V based on conclusion and finally references and bibliography is mentioned.

2. Literature Review

Cybersecurity experts are in high demand since cyber assaults continue to be a major risk for businesses and individuals. The use of machine learning methods to identify and prevent cyber threats in real time has recently emerged as a viable option. The Table 1 provides a brief overview of some studies that have investigated the use of AI approaches for the prediction, prevention and detection of cyber assaults.

Table 1. AI approaches in cyber-attacks prediction, prevention and detection.

No.	Ref.	AI method	AI technique	Attacks	Dataset	Accuracy
1	[17]	IDS model	binary particle swarm optimization (PSO) and k-nearest-neighbor (k-NN) algorithms	DOS attack, PROBE, U2R, R2L	KDD CUP 1999	99.91%
2	[18]	IDS model	Support Vector Machine, k-Nearest Neighbor, and Primal-Dual Particle Swarm Optimization	DoS, Probe, R2L, U2R	KDD99	98.5%
3	[19]	IDS	Zigbee protocol & Naïve bayes algorithm	DDOS	CICDDoS2019	45%
4	[20]	ANN model compared with PSO	Levenberg–Marquardt LM algorithm	UDP Flood, TCP SYN	KDD Cup99, DARPA98	
5	[21]	Features classification	ANN, Naïve Bayes, and Decision Table algorithms	DDOS attacks	UNSW-NB 15 dataset	88.43%
6	[22]	IDM	Grid Search Cross-Validation (GSCV), Radial Basis Function (RBF) kernel of the Support Vector Machine (SVM) classifier	DDoS attack		99.33
7	[23]	DL-IDS	spider monkey optimization (SMO) algorithm and stacked-deep polynomial network (SDPN)	Anomaly detection	NSL-KDD benchmark	99.2%
8	[24]	Deep learning	CNN-MLP CNN-LSTM	APT attacks	CTU-13	98%

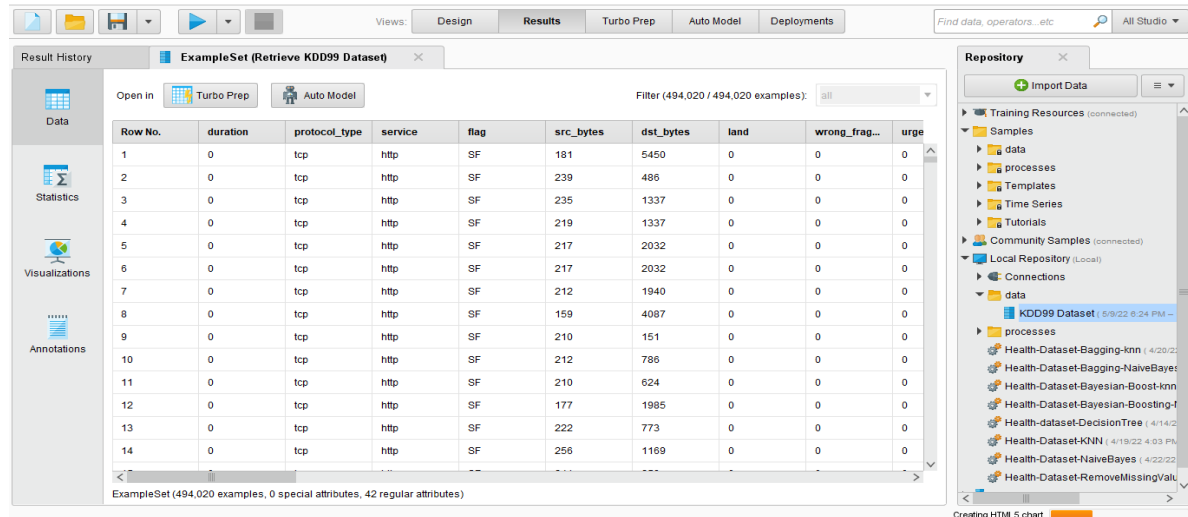
9	[25]	(DL) driven SDN-enabled architecture	LSTM-GRU LSTM-CNN	Denial of Service (DoS), Distributed Denial of Service (DDoS), Infiltration, malware, and botnets attacks	CIDDS-001	99.2%
10	[26]	IDS	Genetic Algorithm Wrapper-Based feature selection and Nave Bayes	Anomaly	NSL-KDD	99.73%
11	[27]	IDS	Decision tree	Cyber attacks	UNSW-NB 15	96.7%
12	[28]	Software Defined Network Function Virtualization (SDNFV) network	conventional network data (DT), Bayesian Network (BayesNet), Naive-Bayes, C4.5, and Decision Table (DT) algorithms	Cyber attacks	AWS honeypot	92.87%
13	[29]	Bot IDS	baptized BotIDS, CNN	Botnet attacks	Bot-IoT	99.94%
14	[30]	SDN based	MLP, CNN, and LSTM	Port scan attack: adversarial attacks, FGSM, JSMA and JSMA-RE	SDN training	98%
15	[31]	adversarial deep learning, Network Security Situation Assessment NSSA	Deep Autoencoder-Deep Neural Network DAENN network, AEDNN+UOSW, LSTM, SVM & DT	Normal, DoS, U2R, R2L, and Probe	NSL-KDD	AEDNN+UOSW has highest accuracy
16	[32]	PCA, RFE	Linear regression, SVM	DDoS	CIC-DDoS2019	99%
17	[33]	PCA, RFE	Linear regression, SVM	DDoS	CIC-DDoS2019	99%
18	[34]	Deep learning – novel approach	Genetic Algorithm (EGA), Deep Autoencoder and a Deep Feedforward Neural Network (DFFNN)	Cyber attacks	CICIDS2017 and UNSW_NB15	35%
19	[35]	Machine learning model, IPS	Cyber physical system, Cognitive machine learning assisted attack detection framework (CML-ADF)	Cyber attacks	Network packets	98.2%
20	[36]	Machine learning	Logistic Regression (LR) algorithm	Dos Attacks-zero-day attacks	CICDoS2019	99.7%
21	[37]	Deep learning	CNN + LSTM	DDos Attacks	CICIDS2017	97.16%
22	[38]	IDS	1D-DCNN, RNN	Cyber attacks	CIC-IDS2017 and CSE-CIC-IDS2018	99.8%
23	[39]	IDS model	K mean algorithm, Anomaly-based-RealTime-Prevention (ARTP) mode	Dos attacks	LLDDOS dataset	85%
24	[40]	Deep learning	DNN	DDoS Attacks	CICDDoS2019	94.5%
25	[41]	Deep learning – Bio inspired	bat algorithm	App-DDOS by HTTP flood	CAIDA	94.8%

3. Methodology

The flow diagram of the methodology is shown in Fig. 4. In this research, the focus is on the ML clustering approaches. Fig. 4 is representing the overall structure of the research. We used KDD99 dataset and applied four different clustering approaches; Boosting Naïve Bayes, SVM, K-Mean and K-Medoids. Further, we divided our work into cyber-attacks prediction and detection. So, we used Boosting Naïve Bayes for cyber-attacks prediction and K-Mean and K-Medoids for cyber-attacks detection.

3.1. Dataset

We used the KDD99 dataset, which is made up of around 4,900,000 single connection vectors with 41 characteristics, each of which is classified as either normal or an attack and has a single attack type. Mostly researchers use KDD99 dataset in IDS and machine learning. Fig. 5. Represents the KDD 99 dataset in RapidMiner.



Row No.	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_frag...	urge
1	0	tcp	http	SF	181	5450	0	0	0
2	0	tcp	http	SF	239	486	0	0	0
3	0	tcp	http	SF	235	1337	0	0	0
4	0	tcp	http	SF	219	1337	0	0	0
5	0	tcp	http	SF	217	2032	0	0	0
6	0	tcp	http	SF	217	2032	0	0	0
7	0	tcp	http	SF	212	1940	0	0	0
8	0	tcp	http	SF	159	4087	0	0	0
9	0	tcp	http	SF	210	151	0	0	0
10	0	tcp	http	SF	212	786	0	0	0
11	0	tcp	http	SF	210	624	0	0	0
12	0	tcp	http	SF	177	1985	0	0	0
13	0	tcp	http	SF	222	773	0	0	0
14	0	tcp	http	SF	256	1169	0	0	0

Figure 4. KDD99 Dataset

4. Results and Discussion

In this section, we describe the experimental results from our research on four different ML clustering approaches.

4.1. Cyber-Attacks Prediction

As we are using KDD99 dataset so we are going to perform classification by SVM support vector machine and Bayesian Boost (Naive Bayes) for the prediction of attacks.

- **Set Role:** To modify the role of one or more attributes, we can utilize the "Set Role" function, selecting "outcome" as the target role or label.
- **Split Data:** This operator used to produce the required number. Here we take 70% for training and 30% for testing.
- **Apply Model:** This executes a model on a given dataset.
- **Performance (Classification):** The operator is utilized to perform statistical analysis and evaluation of the **performance** of classification tasks. It is used to generate a list of performance criteria values related to task of classification, with accuracy being one of them.
- **Bayesian Boosting:** It is based on a meta-algorithm which is useful to enhance the performance by using with other learning algorithm.
- **Naive Bayes:** This Operator generates a Naive Bayes classification model.

4.1.1. Boosting Naïve Bayes Model

Boosting naïve bayes is an ensemble meta-algorithm used for minimizing the bias primarily. It is also a modified machine learning algorithms that enhance the weak learners to strong ones for better conclusions. Boosting is a machine learning technique that involves combining several weak learners to create a strong learner. In the context of the Naive Bayes model, boosting can be used to improve the accuracy of the classifier.

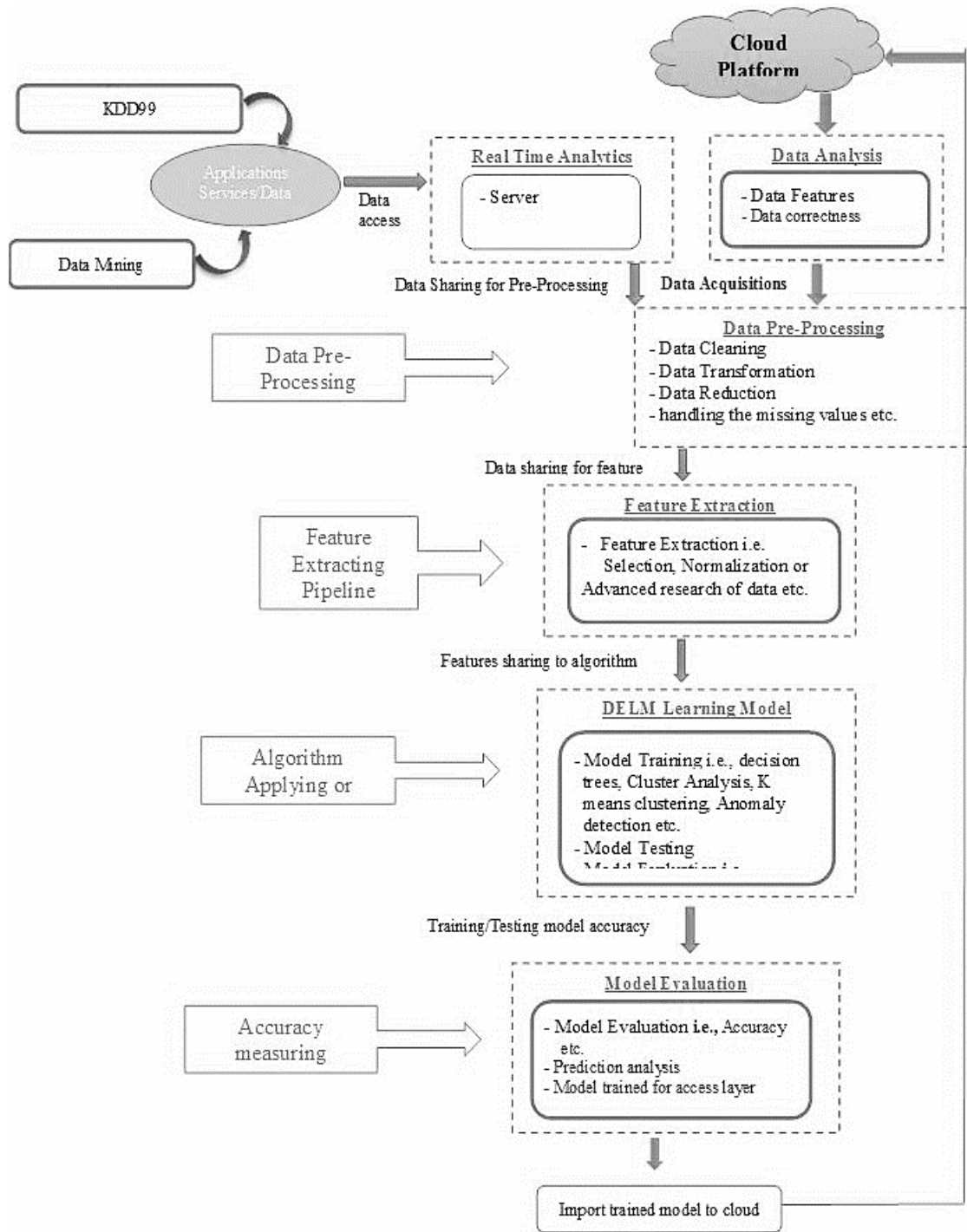


Figure 5. Flow diagram of Methodology

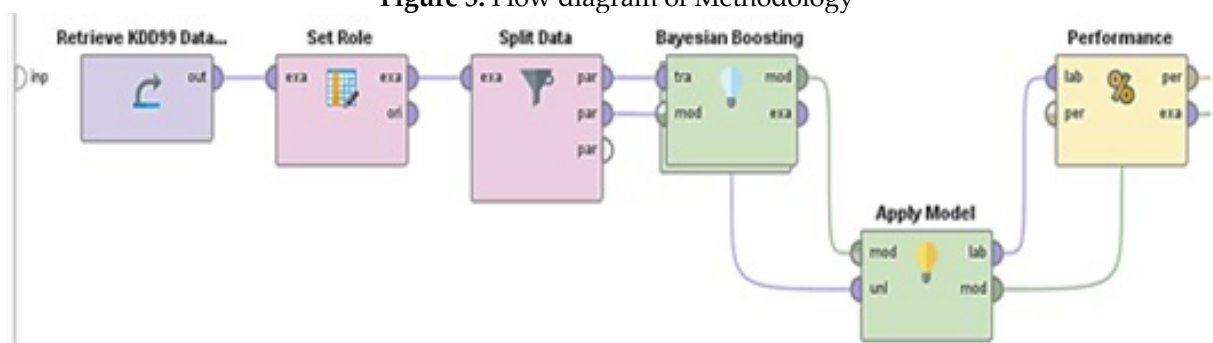


Figure 6. Naive Bayes Process Model

4.1.2. SVM Model



Figure 7. SVM Process Model

4.1.3. Comparison

Table 2. Accuracy of SVM and BNB

Classifier	Accuracy
SVM	99.19%
Boosting Naïve Bayes	92.68%

Hence SVM gives the better results against KDD99 Dataset to predict the cyber-attacks.

4.2. Cyber-Attacks Detection

K-Mean and K-Medoid models are used in the study for cyber-attacks detection.

4.2.1. K-Mean Model

K-means is an algorithm for clustering that combined items into sets of clusters to achieve the desired results. It uses a squared error approach to cluster elements, resulting in high similarity within clusters and dissimilarity between different clusters.

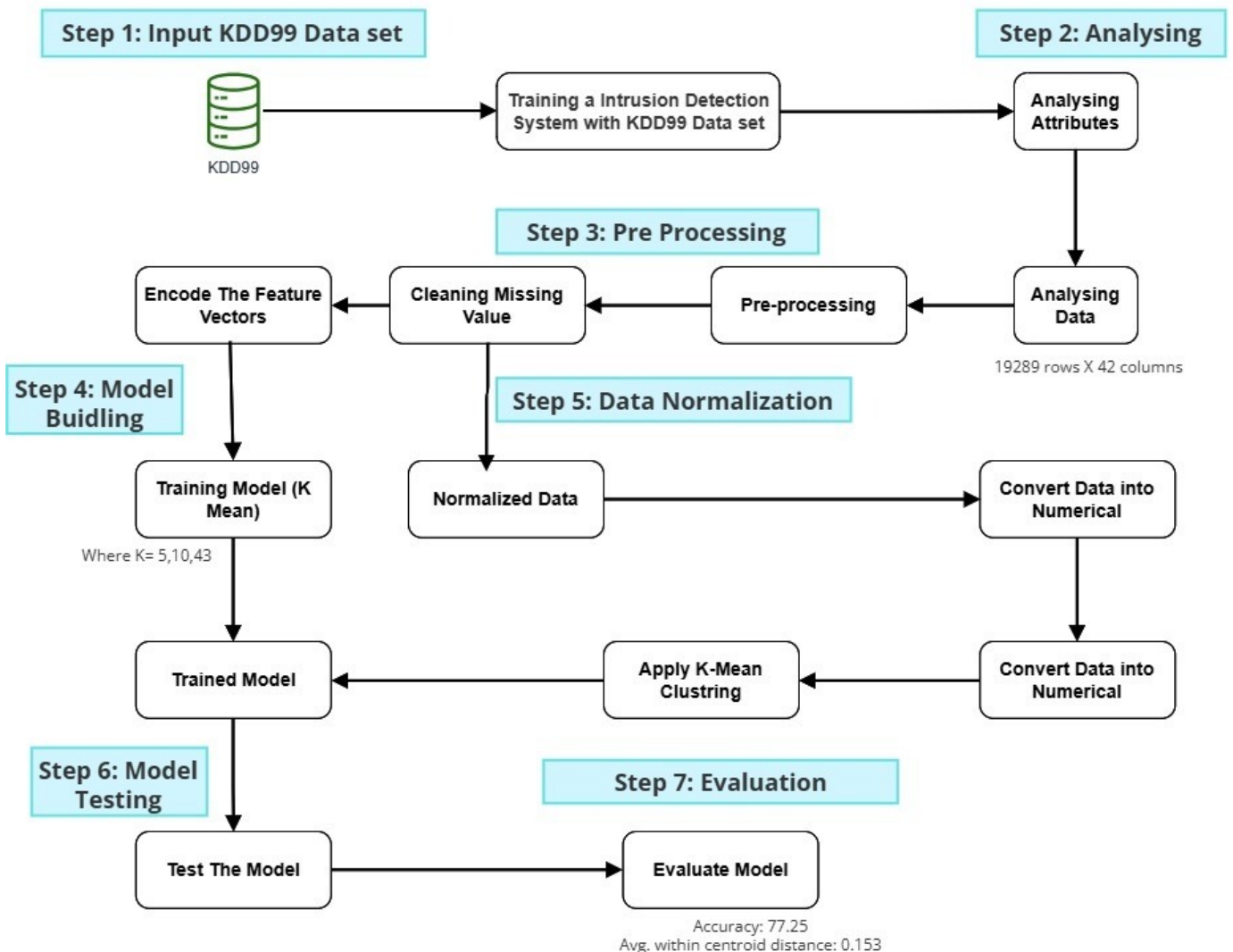


Figure 8. K-Mean Flow diagram

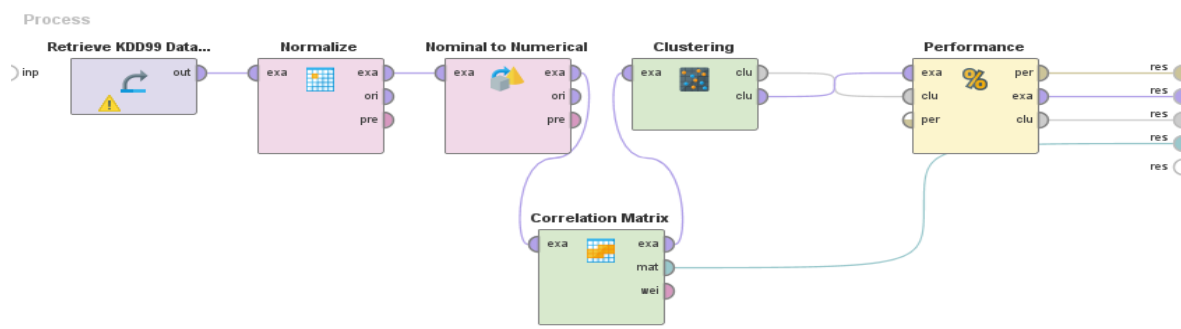


Figure 9. K-Mean Process Model

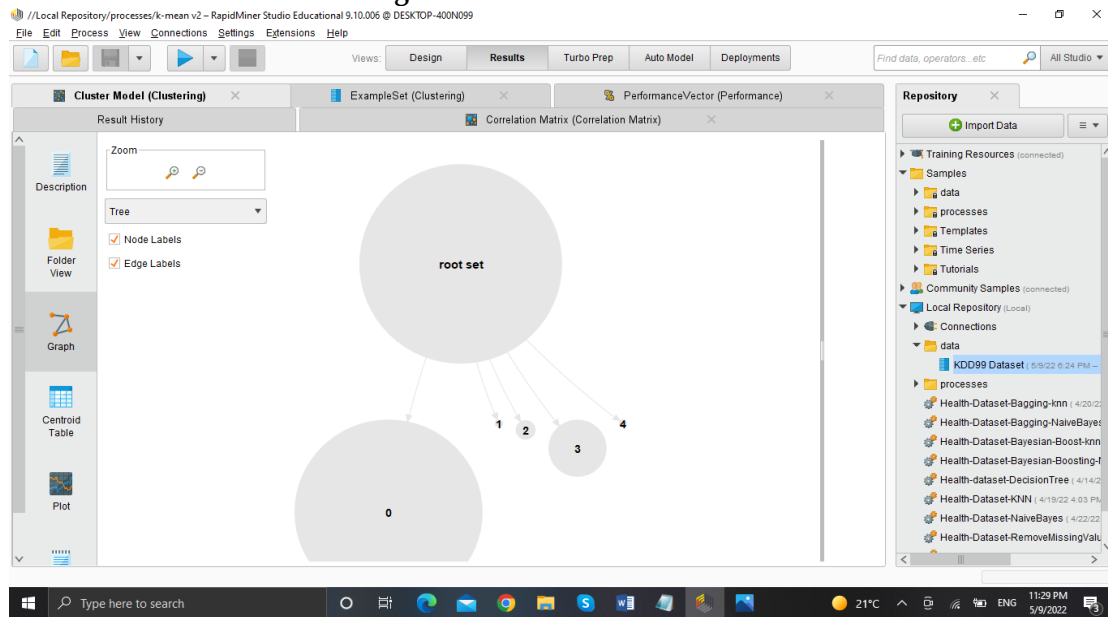


Figure 10. K-Mean clustering if K=5

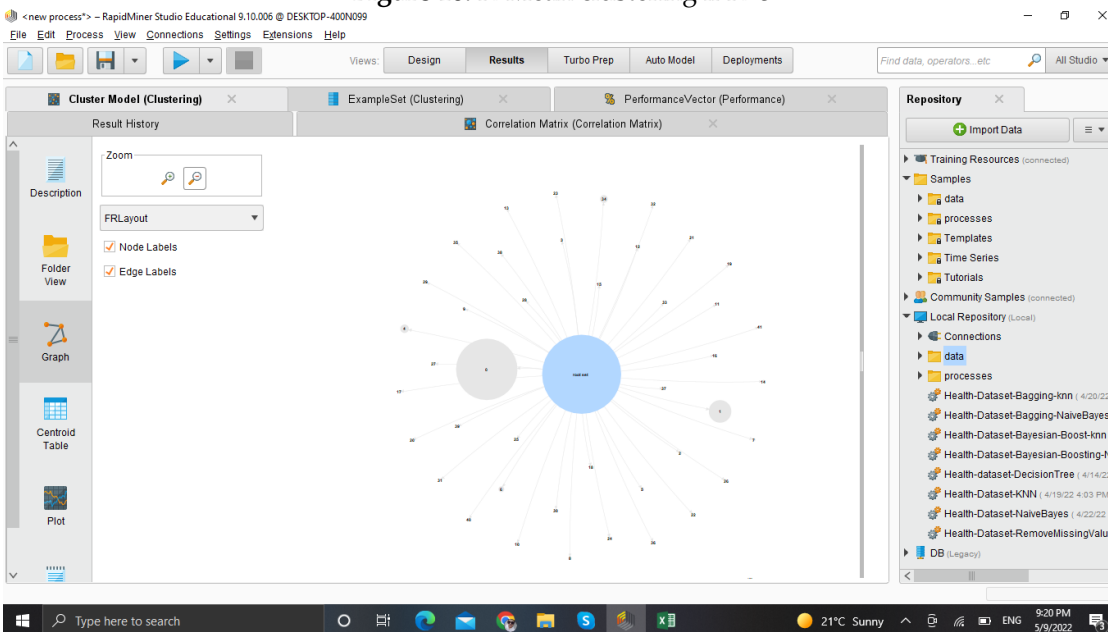


Figure 11. K-Mean clustering if K=43

4.2.2. K-Medoid Model

K-medoids clustering is a variant of K-means that is more resilient to noise and outliers. Instead of using the mean point to represent the cluster center, K-medoids use a genuine point in the cluster. The object in the cluster with the fewest total distances between other places and the closest proximity to the center is called medoid.

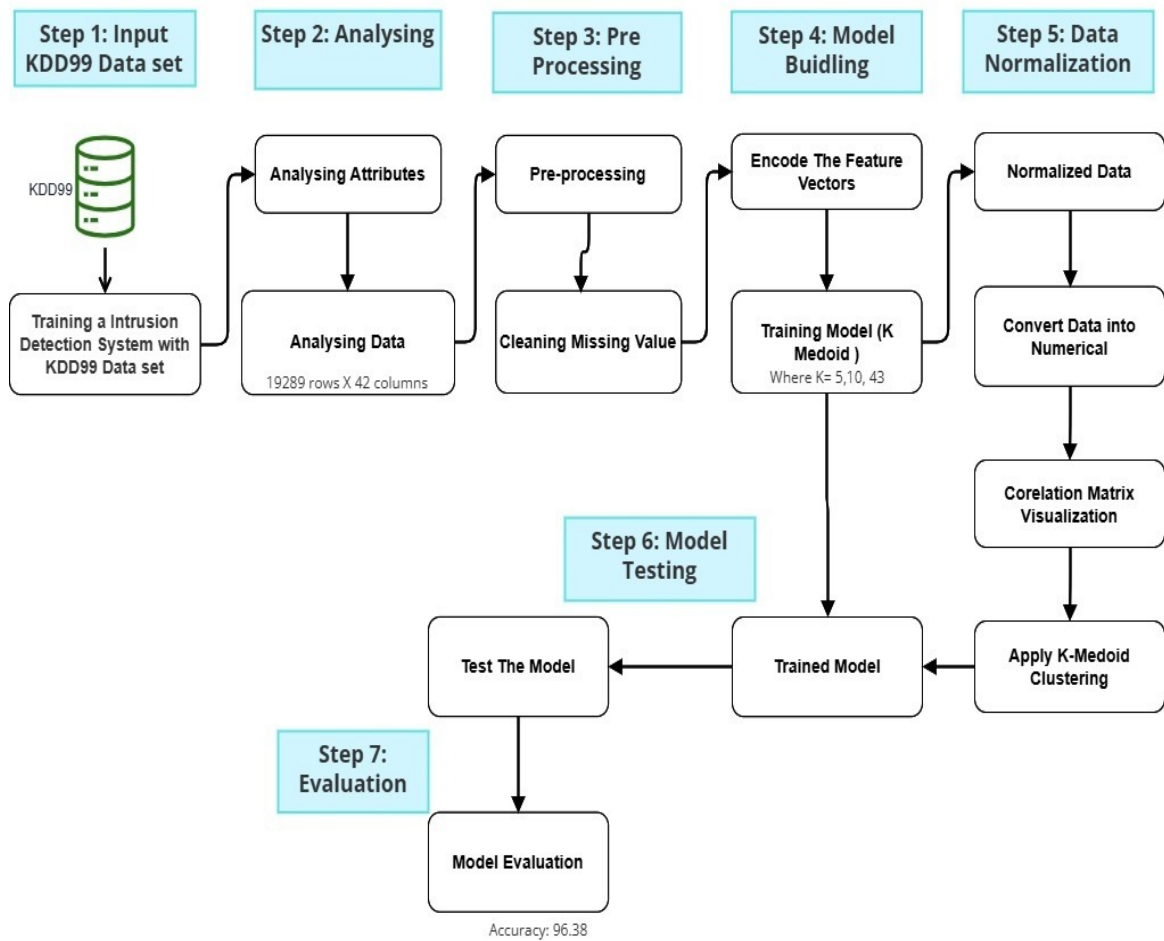


Figure 12. K-Medoid Flow Diagram

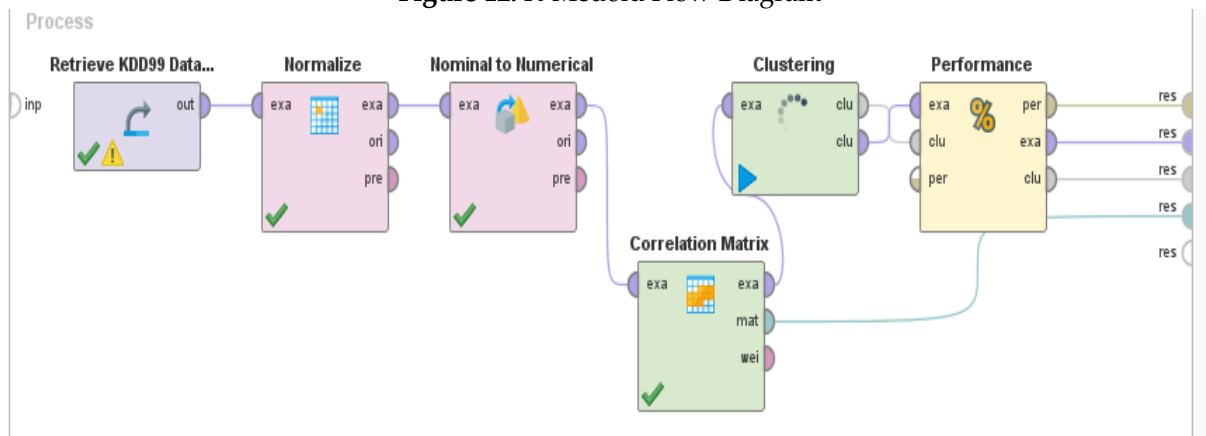


Figure 13. K-Medoid process model

4.2.3. Comparison

Table 3. Accuracy Table of K-Mean and K-Medoid

Clustering	Accuracy
K-Means	77.25%
K-Medoids	96.38%

Table 4. K-Means vs. K-Medoids

K-Means	K-Medoids
K means have cluster dependency.	K medoids have no cluster dependency
K means have k number clusters with dissimilarities.	K medoids have clusters with the least dissimilarities.

K means make clusters with little difference.	K medoids try to make clusters with less difference
K means uses Euclidean distance formula.	K medoids uses Manhattan distance formula
In K means the final cluster is not an actual data point. It is the average of data points in a cluster.	In K medoids the final cluster is an actual data point.

5. Conclusion

Cybersecurity is essential to living in the networked world. We need very precise and state-of-the-art technologies and procedures for attack detection, prevention, and prediction. In order to create effective IDS, we looked at many clustering techniques for cyberattack prediction and prevention in this study. Here, we provide a novel approach to initial medoids selection that outperforms the conventional K-means algorithm in identifying abnormal incursions. The suggested method has its roots in data mining clustering, a well-liked and exciting field of intrusion detection study. It has several drawbacks that need to be addressed further, but it also has a number of benefits over current approaches.

References

1. Social, Índice Rezago. "Internet." Observatorio Social.[citado 22 de diciembre de 2020]. Disponible en: <http://observatorio.ministeriodesarrollosocial.gob.cl> (2020).
2. Al-Sarawi, Shadi, et al. "Internet of things market analysis forecasts, 2020–2030." 2020 Fourth World Conference on smart trends in systems, security and sustainability (WorldS4). IEEE, 2020.
3. Guembe, Blessing, et al. "The emerging threat of ai-driven cyber attacks: A review." *Applied Artificial Intelligence* 36.1 (2022): 2037254.
4. AlDaajeh, Saleh, et al. "The role of national cybersecurity strategies on the improvement of cybersecurity education." *Computers & Security* 119 (2022): 102754.
5. Aulianisa, Sarah Safira, and Indirwan Indirwan. "Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia." *Lex Scientia Law Review* 4.1 (2020): 31-45.
6. Geetha, R., and T. Thilagam. "A review on the effectiveness of machine learning and deep learning algorithms for cyber security." *Archives of Computational Methods in Engineering* 28.4 (2021): 2861-2879.
7. Kilincer, Ilhan Firat, Fatih Ertam, and Abdulkadir Sengur. "Machine learning methods for cyber security intrusion detection: Datasets and comparative study." *Computer Networks* 188 (2021): 107840.
8. Rekha, Gillala, et al. "Intrusion detection in cyber security: role of machine learning and data mining in cyber security." *Advances in Science, Technology and Engineering Systems Journal* 5.3 (2020): 72-81.
9. Landauer, Max, et al. "System log clustering approaches for cyber security applications: A survey." *Computers & Security* 92 (2020): 101739.
10. Al-Daweri, Muataz Salam, et al. "An analysis of the KDD99 and UNSW-NB15 datasets for the intrusion detection system." *Symmetry* 12.10 (2020): 1666.
11. Bogdal, Christian, et al. "Recognition of gasoline in fire debris using machine learning: Part I, application of random forest, gradient boosting, support vector machine, and naïve bayes." *Forensic science international* 331 (2022): 111146.
12. Pisner, Derek A., and David M. Schnyer. "Support vector machine." *Machine learning*. Academic Press, 2020. 101-121.
13. Ikotun, Abiodun M., et al. "K-means clustering algorithms: A comprehensive review, variants analysis, and advances in the era of big data." *Information Sciences* 622 (2023): 178-210.
14. Herman, Emilia, Kinga-Emese Zsido, and Veronika Fenyves. "Cluster analysis with k-mean versus k-medoid in financial performance evaluation." *Applied Sciences* 12.16 (2022): 7985.
15. Camacho, Nicolas Guzman. "The Role of AI in Cybersecurity: Addressing Threats in the Digital Age." *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023* 3.1 (2024): 143-154.
16. Dash, Bibhu, et al. "Threats and opportunities with AI-based cyber security intrusion detection: a review." *International Journal of Software Engineering & Applications (IJSEA)* 13.5 (2022).
17. Syarif, A.R., Gata, W.: Intrusion detection system using hybrid binary PSO and K-nearest neighborhood algorithm. In: 2017 11th International Conference on Information & Communication Technology and System (ICTS). pp. 181–186 (2017). <https://doi.org/10.1109/ICTS.2017.8265667>.
18. Dada, E.G.: A Hybridized SVM-kNN-pdAPSO Approach to Intrusion Detection System. 8, (2017).
19. Masud, I., Kusri, K., Prasetyo, A.B.: Distributed Denial Of Service (DDoS) Attack Detection On Zigbee Protocol Using Naive Bayes Algorithm. *Int. J. Artif. Intell. Res.* 5, (2021). <https://doi.org/10.29099/ijair.v5i2.214>.
20. Gopi, R., Sathiyamoorthi, V., Selvakumar, S., Manikandan, R., Chatterjee, P., Jhanjhi, N.Z., Luhach, A.K.: Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things. *Multimed. Tools Appl.* 81, 26739–26757 (2022). <https://doi.org/10.1007/s11042-021-10640-6>.
21. Azmi, M.A.H., Foozy, C.F.M., Sukri, K.A.M., Abdullah, N.A., Hamid, I.R.A., Amnur, H.: Feature Selection Approach to Detect DDoS Attack Using Machine Learning Algorithms. *JOIV Int. J. Inform. Vis.* 5, 395–401 (2021). <https://doi.org/10.30630/joiv.5.4.734>.
22. Anyanwu, G.O., Nwakanma, C.I., Lee, J.-M., Kim, D.-S.: Optimization of RBF-SVM Kernel using Grid Search Algorithm for DDoS Attack Detection in SDN-based VANET. *IEEE Internet Things J.* 1–1 (2022). <https://doi.org/10.1109/JIOT.2022.3199712>.
23. Otoum, Y., Liu, D., Nayak, A.: DL-IDS: a deep learning-based intrusion detection framework for securing IoT. *Trans. Emerg. Telecommun. Technol.* 33, e3803 (2022). <https://doi.org/10.1002/ett.3803>.
24. Do Xuan, C., Dao, M.H.: A novel approach for APT attack detection based on combined deep learning model. *Neural Comput. Appl.* 33, 13251–13264 (2021). <https://doi.org/10.1007/s00521-021-05952-5>.

25. Ullah, I., Raza, B., Ali, S., Abbasi, I.A., Baseer, S., Irshad, A.: Software Defined Network Enabled Fog-to-Things Hybrid Deep Learning Driven Cyber Threat Detection System. *Secur. Commun. Netw.* 2021, e6136670 (2021). <https://doi.org/10.1155/2021/6136670>.
26. Onah, J.O., Abdulhamid, S.M., Abdullahi, M., Hassan, I.H., Al-Ghusham, A.: Genetic Algorithm based feature selection and Naïve Bayes for anomaly detection in fog computing environment. *Mach. Learn. Appl.* 6, 100156 (2021). <https://doi.org/10.1016/j.mlwa.2021.100156>.
27. Al-Omari, M., Rawashdeh, M., Qutaishat, F., Alshira'H, M., Ababneh, N.: An Intelligent Tree-Based Intrusion Detection Model for Cyber Security. *J. Netw. Syst. Manag.* 29, 20 (2021). <https://doi.org/10.1007/s10922-021-09591-y>.
28. Prabakaran, S., Ramar, R., Hussain, I., Kavin, B.P., Alshamrani, S.S., AlGhamdi, A.S., Alshehri, A.: Predicting Attack Pattern via Machine Learning by Exploiting Stateful Firewall as Virtual Network Function in an SDN Network. *Sensors.* 22, 709 (2022). <https://doi.org/10.3390/s22030709>.
29. Dahou, A., Abd Elaziz, M., Chelloug, S.A., Awadallah, M.A., Al-Betar, M.A., Al-qaness, M.A.A., Forestiero, A.: Intrusion Detection System for IoT Based on Deep Learning and Modified Reptile Search Algorithm. *Comput. Intell. Neurosci.* 2022, e6473507 (2022). <https://doi.org/10.1155/2022/6473507>.
30. De Assis, M.V.O., Novaes, M.P., Zerbini, C.B., Carvalho, L.F., Abrao, T., Proenca, M.L.: Fast Defense System Against Attacks in Software Defined Networks. *IEEE Access.* 6, 69620–69639 (2018). <https://doi.org/10.1109/ACCESS.2018.2878576>.
31. Yang, H., Zeng, R., Xu, G., Zhang, L.: A network security situation assessment method based on adversarial deep learning. *Appl. Soft Comput.* 102, 107096 (2021). <https://doi.org/10.1016/j.asoc.2021.107096>.
32. Bilen, A., Özer, A.B.: Cyber-attack method and perpetrator prediction using machine learning algorithms. *PeerJ Comput. Sci.* 7, (2021). <https://doi.org/10.7717/peerj-cs.475>.
33. Liu, Z., Qian, L., Tang, S.: The prediction of DDoS attack by machine learning. In: *Third International Conference on Electronics and Communication; Network and Computer Technology (ECNCT 2021)*. pp. 681–686. SPIE (2022). <https://doi.org/10.1117/12.2628658>.
34. Ibor, A.E., Oladeji, F.A., Okunoye, O.B., Uwadia, C.O.: Novel adaptive cyberattack prediction model using an enhanced genetic algorithm and deep learning (AdacDeep). *Inf. Secur. J. Glob. Perspect.* 31, 105–124 (2022). <https://doi.org/10.1080/19393555.2021.1883777>.
35. AlZubi, A.A., Al-Maitah, M., Alarifi, A.: Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. *Soft Comput.* 25, 12319–12332 (2021). <https://doi.org/10.1007/s00500-021-05926-8>.
36. Chesney, S., Roy, K., Khorsandroo, S.: Machine Learning Algorithms for Preventing IoT Cybersecurity Attacks. In: Arai, K., Kapoor, S., and Bhatia, R. (eds.) *Intelligent Systems and Applications*. pp. 679–686. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-55190-2_53.
37. Roopak, M., Yun Tian, G., Chambers, J.: Deep Learning Models for Cyber Security in IoT Networks. In: *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. pp. 0452–0457 (2019). <https://doi.org/10.1109/CCWC.2019.8666588>.
38. Rizvi, S., Scanlon, M., McGibney, J., Sheppard, J.: Deep Learning Based Network Intrusion Detection System for Resource-Constrained Environments. *13th EAI Int. Conf. Digit. Forensics Cyber Crime.* (2022).
39. Krishna Kishore, P., Ramamoorthy, S., Rajavarman, V.N.: ARTP: Anomaly based real time prevention of Distributed Denial of Service attacks on the web using machine learning approach. *Int. J. Intell. Netw.* 4, 38–45 (2023). <https://doi.org/10.1016/j.ijin.2022.12.001>.
40. Cil, A.E., Yildiz, K., Buldu, A.: Detection of DDoS attacks with feed forward based deep neural network model. *Expert Syst. Appl.* 169, 114520 (2021). <https://doi.org/10.1016/j.eswa.2020.114520>.
41. Sreeram, I., Vuppala, V.P.K.: HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm. *Appl. Comput. Inform.* 15, 59–66 (2019). <https://doi.org/10.1016/j.aci.2017.10.003>.
42. Khan, I. U., Khan, Z. A., Ahmad, M., Khan, A. H., Muahmmad, F., Imran, A., & Hamid, M. K. (2023, May). Machine Learning Techniques for Permission-based Malware Detection in Android Applications. In *2023 9th International Conference on Information Technology Trends (ITT)* (pp. 7-13). IEEE.
43. Shah, A. M., Aljubayri, M., Khan, M. F., Alqahtani, J., Sulaiman, A., & Shaikh, A. (2023). ILSM: Incorporated Lightweight Security Model for Improving QOS in WSN. *Computer Systems Science & Engineering*, 46(2).